

AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions and listings of claims in the application:

1 - 94. (Canceled)

95. (Previously Presented) An information distribution system for distributing predetermined content data from an information sending device to an information receiving device,

said information sending device comprises:

first storing means for storing content data that is prohibited from being played by an information receiving device that does not include a content key;

second storing means for storing content data that is permitted to be played by an information receiving device that does not include the content key;

sending end controlling means for encrypting said content data with a content key, and encrypting the content key with an individual key specific to said information sending device; and

sending means for sending an encrypted individual key by encrypting said individual key with one of a plurality of distribution keys, each distribution key corresponding to a predetermined time period, to said information receiving device together with said content data encrypted with said content key and a content key encrypted with said individual key, and

said information receiving device comprises:

receiving means for receiving said content data encrypted with said content key and said content key encrypted with said individual key together with said encrypted individual key; and

receiving end controlling means for decrypting said individual key with one of said plurality of distribution keys, decrypting said content key with the decrypted individual key, and decrypting said content data with the decrypted content key; and

allowing decryption of said individual key within the predetermined time period associated with said distribution key, independent of a connection during said predetermined time period associated with said distribution key.

96. (Previously Presented) An information distribution method for distributing predetermined content data from an information sending device to an information receiving device, wherein said method comprises:

a first storing step for storing content data that is prohibited from being played by an information receiving device that does not include a content key;

a second storing step for storing content data that is permitted to be played by an information receiving device that does not include the content key;

a sending step of encrypting said content data with a content key, encrypting the content key with an individual key specific to said information sending device, and sending an encrypted individual key made by encrypting said individual key with one of a plurality of distribution keys, each distribution key corresponding to a predetermined time period, to said information receiving device together with said content data

encrypted with said content key and a content key encrypted with said individual key, by said information sending device;

a decrypting step of receiving said content data encrypted with said content key and said content key encrypted with said individual key together with said encrypted individual key, decrypting said individual key with one of said plurality of distribution keys, decrypting said content key with the decrypted individual key, and decrypting said content data with the decrypted content key, by said information receiving device; and

allowing decryption of said individual key within the predetermined time period associated with said distribution key, independent of a connection during said predetermined time period associated with said distribution key.

97. (Previously Presented) An information sending device for sending predetermined content data to an information receiving device, said device comprising:

first storing means for storing content data that is prohibited from being played by an information receiving device that does not include a content key;

second storing means for storing content data that is permitted to be played by an information receiving device that does not include the content key;

sending end controlling means for encrypting said content data with a content key, and encrypting the content key with an individual key specific to said information sending device;

sending means for sending an encrypted individual key made by encrypting said individual key with one of a plurality of distribution keys, each distribution key corresponding to a predetermined time period, to said information receiving means

together with said content data encrypted with said content key and said content key encrypted with said individual key; and

allowing decryption of said individual key within the predetermined time period associated with said distribution key, independent of a connection during said predetermined time period associated with said distribution key.

98. (Original) The information sending device according to Claim 97, characterized in that said sending end controlling means encrypts said content key with said individual key supplied from the outside together with said encrypted individual key.

99. (Original) The information sending device according to Claim 98, characterized in that said sending means sends said encrypted individual key made by encrypting said individual key with said distribution key that is updated periodically, which is supplied from the outside, to said information receiving device together with said content data encrypted with said content key and said content key encrypted with said individual key.

100. (Original) The information sending device according to Claim 99, characterized in that said sending means sends said encrypted individual key appropriate to an update period, in said encrypted individual key for a plurality of periods given together in advance to said information receiving device together with said content data encrypted with said content key and a content key encrypted with said individual key.

101-103. (Canceled)

104. (Previously Presented) An information sending method for sending predetermined content data to an information receiving device, wherein said method comprises:

a first storing step for storing content data that is prohibited from being played by an information receiving device that does not include a content key;

a second storing step for storing content data that is permitted to be played by an information receiving device that does not include the content key;

a encrypting step of encrypting said content data with a content key, and encrypting the content key with an individual key specific to said information sending device;

a sending step of sending an encrypted individual key made by encrypting said individual key with one of a plurality of distribution keys, each distribution key corresponding to a predetermined time period, to said information receiving device together with said content data encrypted with said content key and said content key encrypted with said individual key; and

allowing decryption of said individual key within the predetermined time period associated with said distribution key, independent of a connection during said predetermined time period associated with said distribution key.

105. (Original) The information sending method according to Claim 104, characterized in that in said encrypting step, said content key is encrypted with said individual key supplied from the outside together with said encrypted individual key.

106. (Original) The information sending method according to Claim 105, characterized in that in said sending step, said encrypted individual key made by encrypting said individual key with said distribution key that is updated periodically, which is supplied from the outside, is sent to said information receiving device together with said content data encrypted with said content key and a content key encrypted with said individual key.

107. (Original) The information sending method according to Claim 106, characterized in that in said sending step, said encrypted individual key appropriate to an update period, in said encrypted individual key for a plurality of update periods given together in advance, is sent to said information receiving device together with said content data encrypted with said content key and a content key encrypted with said individual key.

108-110. (Canceled)

111. (Previously Presented) A program storing medium for storing an information sending method, said method comprising:

a first storing step for storing content data that is prohibited from being played by an information receiving device that does not include a content key;

a second storing step for storing content data that is permitted to be played by an information receiving device that does not include the content key;

an encrypting step of encrypting predetermined content data with a content key, and encrypting the content key with an individual key specific to an information sending device;

a sending step of sending an encrypted individual key made by encrypting said individual key with one of a plurality of distribution keys, each distribution key corresponding to a predetermined time period, to said information receiving device together with said content data encrypted with said content key and a content key encrypted with said individual key; and

allowing decryption of said individual key within the predetermined time period associated with said distribution key, independent of a connection during said predetermined time period associated with said distribution key.

112. (Original) The program storing medium according to Claim 111, characterized in that in said encrypting step, said content key is encrypted with said individual key supplied from the outside together with said encrypted individual key.

113. (Original) The program storing medium according to Claim 112, characterized in that in said sending step, said encrypted individual key made by encrypting said individual key with said distribution key that is updated periodically, which is supplied from the outside, is sent to said information receiving device together with said content data encrypted with said content key and a content key encrypted with said individual key.

114. (Original) The program storing medium according to Claim 113, characterized in that in said sending step, said encrypted individual key appropriate to an update period, in said encrypted individual key for a plurality of update periods given together in advance, is sent to said information receiving device together with said

content data encrypted with said content key and a content key encrypted with said individual key.

115-147. (Canceled)

148. (Previously Presented) An information distribution system for sending content data encrypted with a predetermined content key from an information sending device to an information receiving device,

said information sending device comprises:

first storing means for storing content data that is prohibited from being played by an information receiving device that does not include a content key;

second storing means for storing content data that is permitted to be played by an information receiving device that does not include the content key;

sending end controlling means for encrypting said content key with an individual key specific to said information sending device; and

sending means for sending at least said content key encrypted with said individual key, and an encrypted individual key made by encrypting said individual key with one of a plurality of distribution keys, each distribution key corresponding to a predetermined time period, to said information receiving device, and

said information receiving device comprises:

receiving means for receiving at least said content key encrypted with said individual key and said encrypted individual key; and

receiving end controlling means for decrypting said individual key with one of said plurality of distribution keys, decrypting said content key with the decrypted

individual key, and storing the decrypted content key, before said distribution key is updated, thereby making it possible to decrypt said content after said distribution key is updated.

149. (Previously Presented) An information distribution method for sending content data encrypted with a predetermined content key from an information sending device to an information receiving device,

wherein said method comprises:

a first storing step for storing content data that is prohibited from being played by an information receiving device that does not include a content key;

a second storing step for storing content data that is permitted to be played by an information receiving device that does not include the content key;

a sending step of encrypting said content key with an individual key specific to the information sending device, and sending at least said content key encrypted with said individual key, and an encrypted individual key made by encrypting said individual key with one of a plurality of distribution keys, each distribution key corresponding to a predetermined time period, to said information receiving device, by said information sending device; and

a storing step of receiving at least said content key encrypted with said individual key, and said encrypted individual key, and decrypting said individual key with one of said plurality of distribution keys, decrypting said content key with the decrypted individual's key, and storing the decrypted content key before said distribution key is

updated, thereby making it possible to decrypt said content after said distribution key is updated, by said information receiving device.

150-218. (Canceled)